Privacy Impact Assessment

Integrated Acquisition System

January 5, 2004

Revision Log

Revision #	Description	Issue Date	Request By	Page #
0	Privacy Impact Assessment for the Integrated Acquisition System Initiative	8/8/2003	OPPM PSD	All Sections

Table of Contents

Privacy Impact Assessment for the Integrated Acquisition System Initiative

Background

This is the Privacy Impact Assessment for the Integrated Acquisition System (IAS) Initiative. The IAS is a suite of systems that is used for administrative acquisition management of the United States Department of Agriculture (USDA). The IAS is comprised of two key components, a) requisition management and b) contracts management. This Privacy Impact Assessment applies to the whole suite of systems in the Foundation Financial Information System Initiative.

Data in the System

1. Generally describe the information to be used in the system in each of the following categories: Employee, Other.

The data contained in the IAS system can be divided into two categories: seed data, which is that data needed to support all functions of the system, and transaction data, which is that data created by users in using the system. The seed data is divided into four primary categories: user data, vendor information, account code information, and other referential data needed to support the functions of the system. Other referential data refers to enterprise payment terms, office addresses, product service codes, and units of measure. Transactional data will be transactions created by the user and will consist of documents and transactions. The documents created are requisitions and awards. The transactions created are requisition approvals, award approvals, receipt entries, and invoice entries and associated approvals.

2. What are the sources of the information in the system?

Sources of USDA information for IAS originates from the USDA agencies acquisition and budget execution transactions/documents, such as contracts, statements of work, requisitions, etc. entered into the IAS system.

a. What files and databases are used?

Each agency implemented into IAS shares a common database that is logically separated through the use of data and user profiles. IAS agencies configurations are developed and implemented during agency configuration workshops. IAS agencies share a common database that contains enterprise level data such as vendor information, common clauses, etc., and also contains agency specific information and data. All IAS data, enterprise and/or agency level, is physically located in a common Oracle database system.

b. What Federal Agencies are providing data for use in the system?

There are currently 2 USDA agencies that are implemented using IAS. Food and Nutrition Service (FNS) and Rural Development have completed their agencies' rollout to implement IAS. The Forest Service has implemented the solution to a limited user base. The Natural Resource Conversation Service (NCRS) and the Food Safety Inspection Services (FSIS) is in the process of implementing IAS and will complete its rollout by the end of 1st quarter FY'04. Additional agencies are planned for implementation during FY2004 including, but not limited to, the Animal Plant Health Information Service (APHIS), the Agricultural Research Service, etc.

c. What State and Local Agencies are providing data for use in the system?

There are no state or local agencies that are providing data for use with IAS

d. What other third party sources will data be collected from?

Not Applicable

e. What information will be collected from employees, commercial vendors and agencies using the system?

To obtain access to the IAS, Employees provide employee name, employee work location, employee work phone number, employee work electronic mail (e-mail) address, and agency requisition/contracts approver name(s) via IAS user data templates, through the IAS Help Desk, and in some cases may be updated through the user preferences in the system.

USDA Agencies using IAS provide agency specific templates, miscellaneous data, and workflow prior to rollout during Agency Configuration Sessions. Once implemented, data may be updated through the IAS Help Desk.

Commercial vendors data in IAS will be obtained from the vendor's FFIS record, which includes address and contact information. The FFIS will be considered the system of record for all vendor data.

3. a. How will data collected from sources other than USDA records be verified for accuracy?

GSA will provide FAC updates to the FAR as well as NAICS and Product Service Codes to the vendor. Agency team members responsible for reviewing and utilizing the provided updates will verify the collected data using multiple mechanisms such as agency reports as well as direct queries to the IAS.

b. How will data be checked for completeness?- Discuss Data Loading Macros with the configuration team

There is a series of checks and edits that IAS performs to ensure that all the data elements are in place in any incoming data. It also reconciles the number of records that were staged to process through with the number actually processed to ensure there is a match.

c. Is the data current? How do you know?

The only data that may not be current in IAS is non-USDA data such as FAR clauses, NAICS, or PSCs. Users keep their information current through system preferences or the IAS Help Desk. The IAS provides standard reports that can be viewed on-line or in paper form.

4. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes. There is systems documentation for the core tables of the system, IAS user guides for the different modules in the system, training manuals developed for

agency training, security manuals that cover the security tables and Configuration Requirement Documents (CRD's). IAS data element descriptions can be found in:

- Oracle eBusiness Electronic Technical Reference Manual (eTRM) – provides details on the complete Data dictionary of Oracle E-Business Suite., including lists of Tables, Indexes, Columns, etc.
- Oracle iProcurement Implementation Guide Release 11i,
- Compusearch Prism System Setup Systems Administrators Guide, and
- Compusearch Prism System Configuration Guide.

There is also documentation from any enhancements done to the system where a data element is changed or functionality has been modified in the form of release notes. The USDA and agencies also have systems that interface with IAS and this is documented in requirements, designs, testing documents and operations manuals.

Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

IAS Users will have access to the data in the system based on job function and the need-to-know the information. They will be located throughout the USDA agencies, at the USDA's National Information Technology Center, and the National Finance Center. Users are allowed to enter documents and are given the average override level in order to override errors that are less severe and that may occur more often. Security profiles are set up for users to ensure that internal controls and separation of duties are maintained. Sensitive information is restricted from users if there is no valid job-related need for the information to perform the duties of their position. If job duties include providing reports, then users will have access to the required data to run queries against the data.

Managers within the agencies will have access that is based on their job function and the need- to- know the information. They have the ability to approve documents that require approvals, but they are not able to approve documents they enter themselves. They have the highest override authority in case of severe errors that need to be overridden.

System Administrators, which are the Functional Administrators and the Security Administrator in the IAS, have access to the data to perform their job functions. Functional Administrators set parameters for the nightly cycle, check and make changes as necessary to the reference tables in the system to ensure data integrity,

and review system reports to ensure the system is in balance. Security Administrators manage the security tables within the IAS. It is their job function to manage the users authority to update tables within the IAS, ensure the settings on the security tables reflect internal controls and monitor the system logs to check for unauthorized access, overrides and approvals.

The IAS Operations team has access to maintain the system databases and files for the IAS. This requires that high-level access be given based on the job function. Their authority includes changing programs, modifying table structure, managing the servers, and processing files in the IAS. The systems developers also have appropriate access to view the data to ensure it is correct. Access is only granted after appropriate background investigations have been completed for this sensitive position. These users are located at the Office of the Chief Information Officer George Washington Carver Center (GWCC) and the Office of the Chief Information Officer National Information Technology Center.

The USDA also has contractors that have access to the IAS system. They have access that is limited to the functions set forth in the contract. The contractors perform various roles based on their function including applications configuration, application support, and operational support. Contractors undergo background checks before they are allowed to access any data within the system.

Access to all systems is protected by authentication, authorization, encryption of passwords, and password aging. Security background investigations are required of all users and contractors. All users, including contractors, have had security briefings about system security rules and must sign a document confirming that they understand the rules.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Once a user has completed the background investigation required for Federal employment or being a contractor to the Federal Government, then access is granted based on job function and the need-to-know principle. A user signs a document (AD 1143) acknowledging that they have read and understand the system's security rules before access is granted. This document is kept on file with an original signature. The Security Administrator assigns a profile to the user based on their job functions after the request is signed. These profiles have been set up to provide access to only the data and application functions necessary to perform their job functions. Access to all IAS functions and data is managed through the application of standard security groups and user profiles.

The Security Administrator will monitor the systems security audit trail logs and reports to management, any types of unauthorized access attempts, overrides or approvals.

3. Will users have access to all the data on the system or will the users access be restricted? Explain.

A user's access will be restricted based on job function within the agency. A profile used on the users ID within the system will determine what data the user can view in the IAS. It is the responsibility of the users manager and the Security Administrator to ensure the proper paperwork is filled out and signed and that the right profile is attached to the user. Access to all IAS functions and data is managed through the application of standard security groups and user profiles.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?

The profile on the user's ID determines what can be viewed. If there is not a need-to-know on certain data elements then the user will be restricted from seeing that data. To monitor this there will be quarterly reviews conducted to see who has access within the system. Agency Security and System Administrators determine if the user is still employed with the agency and if not that user is deleted from the system. They also monitor to see if job duties have changed, and when appropriate request a change to their profile to ensure the proper profile is attached. The system also keeps logs of security violations. These logs are monitored and any trends in violations are reported to management.

5. a. Do other systems share data or have access to data in this system? If yes, explain.

Not Applicable. The IAS system does not interface with any USDA legacy systems at this time. In FY2004 the IAS will interface with the Foundational Financial Information System (FFIS).

b. Who will be responsible for protecting the privacy rights of the employees affected by the interface?

All users, agencies and the Office of Procurement and Property Management (OPPM) have this responsibility. The IAS PMO has implemented numerous controls within the IAS solution including encryption and restricted access to data and functionality to protect employee's privacy data. These controls will be extended to the IAS-FFIS interface when it is implemented.

6. a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

FPDS Data from IAS will be shared with GSA. This is currently done by extracting the FPDS file from IAS and uploading it to GSA's FPDS Reporting System.

b. Who will be responsible for assuring proper use of the data?

The agencies, the OPPM, users, managers, contractors, and Functional and Security Administrators all have the responsibility to assure the proper use of the data.

Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

The use of the data in IAS is necessary to ensure reliable and accurate USDA-wide, procurement-related financial information and data. It is also important to support acquisition management activities of the agencies within the USDA. Information collected on individuals and business is also necessary for the prompt payment of agency obligations.

2. a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No, the system will not derive new data about an individual or individuals accessing the IAS.

b. Will the new data be placed in the individuals record?

Not applicable.

c. Can the system make determinations about vendors or employees that would not be possible without the new data?

The system does not provide the ability to make any determinations about employees that is not otherwise possible. Through management reporting tools present in IAS, the solution allows users to see how many solicitations were sent to given vendors and how many responses were received. The system also allows users to see how many awards were given to vendors. Managers may also use the reporting capability in IAS to assign award activities based on buyer workloads. All of this aforementioned functionality is based on a users agency.

d. How will the new data be verified for relevance and accuracy?

Not applicable.

3. a. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

There is restricted access on the systems and monitoring of any attempts at unauthorized access. Access to all IAS functions and data is managed through the application of standard security groups and user profiles.

b. If the processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Yes, there is a set of internal controls and reviews conducted to prevent unauthorized access. Protection of data is a multi-layered approach. There is restricted access based on the user ID within the system, monitoring by Security Administrators and Management for unauthorized access attempts, and security audits are conducted on the system.

4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain?

Yes, acquisition data can be retrieved by personal identifier, user name, for activity reporting data. The information contained in the IAS can retrieve data on this system by running reports and online viewing. Access to this data is restricted by role, whether data is agency or enterprise specific, and a need-to-know basis.

What are the potential effects on the due process rights of employees of:

consolidation and linkage of files and systems; derivation of data; accelerated information processing and decision making; use of new technologies?

IAS data is more restricted within each agency. Data processed is relevant acquisition accounting events. Access to IAS data is restricted to users based on agency assigned roles in accordance with the respective employees requirements to perform their assigned tasks.

How are the effects to be mitigated?

Security policy, procedures, oversight and reviews are implemented to mitigate the effects in all these systems. The applicable controls implemented within the IAS are in compliance with JFMIP, USDA OCIO Cyber Security guidance, NIST and FISCAM requirements.

Maintenance of Administrative Controls

1. a. Explain how the system and its use will ensure equitable treatment of employees.

Not applicable.

b. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The IAS systems are operated at one site, but they will be accessed across the United States and some foreign sites. All IAS data accessed will be located at the IAS host site – The Office of the Chief Information Officer (OCIO) National Information Technology Center (NITC) in Kansas City, MO. The IAS disaster recovery site is located at the NITC George Washington Carver Center (GWCC) located in Beltsville, MD. IAS security criteria, rules, procedures and documentation are used by all users regardless of location to ensure universal compliance with security policy.

c. Explain any possibility of disparate treatment of individuals or groups?

Not applicable.

2. a. What are the retention periods of data in this system?

Data in the IAS will accumulate over time and will include historical data. Files/data will be kept for a minimum of six years to comply with Federal regulations.

b. What are the procedures for eliminating the data at the end of the retention? Where are the procedures documented?

No files or data have been eliminated because the system is newly implemented. Data archiving processes are in the concept phase and will be developed and implemented in accordance with Federal regulations and requirements.

c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

Audits require that data be retained. The data is accurate because the checks the system does will show if the system is out of balance.

3. a. Is the system using technologies in ways that the USDA has not previously employed?

Yes. The USDA is using a USDA enterprise-wide web-based acquisition system for the first time that standardizes the processing and handling of procurement data. The IAS is a COTS based solution comprised of front-end web based technologies that are integrated with a standard database approach.

b. How does the use of this technology affect employee privacy?

There is sensitive information on the systems but security measures are taken to ensure that information is kept private. All IAS telecommunications are encrypted using Secure Sockets Layer (SSL v2) to protect data. The agencies that

have been implemented into the IAS use security profiles to keep sensitive information private and have encrypted passwords that have to be changed on demand of the system. All IAS data, including accounts and passwords, are encrypted in the IAS Oracle database. Multiple levels of USDA firewalls and intrusion detection systems are utilized to control access and monitor communications to the IAS. The only data stored in IAS about a user includes their gender and full name, but it does not display this information anywhere.

4. a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The system will allow individuals, e.g. IAS security administrators, agency security administrators, with the appropriate amount of access to run reports which detail who has logged into IAS. This report does not differentiate a user by location nor does it list a users name, as only the User IDs appear on the list.

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

No.

c. What controls will be used to prevent unauthorized monitoring?

The IAS does not provide any capability to monitor any employee activity outside of assigned IAS acquisition related activities. Only IAS system administrators and agency IAS administrators will be able to view the status of employee work activity related to their assigned acquisition tasks.

5. a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.

The IAS is currently not interfaced with the USDA FFIS system and therefore is not under any applicable System of Record (SOR) notice. The IAS and FFIS interface is expected to be implemented during FY2004 and at that time will be subjected to the applicable SOR notices for FFIS and IAS. These SOR's will be identified at that time.

b. If the system is being modified, will the SOR require amendment or revision? Explain.

Yes, because a new system will replace the legacy system a revision to the applicable SOR's will probably be required.